REMARKS

Claims 64-94 and 109 are pending in the application.

In paragraph 4 on page 2 of the Office Action, claims 64-94 and 109 were under 35

U.S.C. § 112, first paragraph as failing to comply with the written description requirement.

Applicant respectfully traverses the rejections.

The Final Office Action states that claims 64, 80 and 109 recite language not

supported by the specification as filed. More particularly, the Final Office Action states

that the specification fails to disclose "anonymously intercepting and capturing."

Applicant respectfully submits that in the "Brief Summary of the Invention" on

page 3, the method and system are described as anonymously profile Web users . . . uses

behavioral information preferably collected . . . to anonymously profile their interests and

demographics." Further, the abstract states that "[t]he system uses behavioral

information preferably collected at the users' point of connection to the Internet to

anonymously profile their interests and demographics." Still further, on page 6, line 6,

the specification states that the ISP POP server 16 captures URL page requests from

individual client machines 10 for use in user profiling" [anonymously profiling users

according to the summary and abstract]. Figure 3 is described as illustrating the data

collection component of the system, which resides at the POP server 16 and gathers data

used in user profiling. The data collection component captures URL requests from

clients, associates the requests with particular-clients, and stores the data in a database

(the UserID and URL database 30). The data collection component includes a sniffer 31

that monitors user-to-Internet traffic. When the sniffer 31 detects an outgoing Web page

request from a client 10, it captures the associated packets, extracts the actual URL

request, and stores it in the database 30 along with the client's IP address.

Thus, Applicant respectfully submits that the specification discloses anonymously

intercepting and capturing as performed by the sniffer 31 in the ISP POP server 16.

In addition, the Final Office Action states that the specification fails to disclose

"prior to each packet from the Web user being routed over the Internet."

However, As shown in Fig. 3, the POP server 16 is disposed prior to the Internet

and thus the sniffer 31 captures an outgoing Web page request "prior to each packet from

the Web user being routed over the Internet."

Thus, Applicant respectfully submits that the specification discloses "prior to each

packet from the Web user being routed over the Internet."

Still further, the Final Office Action states that the specification fails to disclose

analyzing each of the intercepted and captured packets to identify packets having headers

associated with Web page requests, extracting, at the ISP POP, a current IP address of the

Web user from the headers identified to be associated with Web page requests, processing

the current IP address extracted from the captured headers to correlate the current IP

address extracted from the captured headers with a permanent anonymous user identifier

using a cross-reference table at the ISP POP, and associating each extracted URL with the

permanent anonymous user identifier correlated with the current IP address extracted from

the captured headers.

However, the specification at page 7, lines 12-20, describes the sniffer capturing

packets. Those skilled in the art understand that packets consist of at least a header and a

payload. In addition, those skilled in the art understand that a Web page request is an

HTTP request, which is based on the HTTP request/response protocol. Those skilled in the

art understand that the request includes at least the Source IP address and the Source port.

The specification states that an IP address to anonymous user ID (AID) cross-reference

table is queried to obtain a userID. Those skilled in the art will also understand that a

request packet will include Destination IP address and the Requested URI. Those skilled in

the art understand that all of this information is provided in the headers of an HTTP Web

page request. All of this information is elementary to understanding HTTP.

Thus, the packets are analyzed to determine which packets are associated with

HTTP Web page requests by analyzing the headers that are extracted from packets and the

IP address obtained from the headers is correlated with an associated client by querying an

IP address to anonymous user ID (AID) cross-reference table.

Finally, the Final Office Action states that the specification fails to disclose "for

each permanent anonymous user identifier correlated with the current IP address

extracted from the captured headers" and "storing the URL of the requested Web page

and the permanent anonymous user identifier correlated with the current IP address

extracted from the captured headers at the ISP POP."

However, the specification at page 7, lines 19-20, describes the User ID and the

URL information are stored in the database.

Accordingly, Applicant respectfully submits that the claims meet the written

description requirements of 35 U.S.C. § 112, first paragraph.

On the basis of the above amendments and remarks, it is respectfully submitted that the claims are in immediate condition for allowance. Accordingly, reconsideration of this application and its allowance are requested.

If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Attorney for Applicant, David W. Lynch, at 865-380-5976. If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 13-2725 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

Merchant & Gould
P.O. Box 2903
Minneapolis, MN 55402-0903
(865) 380-5976

94140
PATENT TRADEMARK OFFICE

By: _____
Name: David W. Lynch
Reg. No.: 36,204

5